CSC-EPL-87/002

(2)

NATIONAL COMPUTER SECURITY CENTER

FINAL EVALUATION REPORT OF ENIGMA LOGIC, INC. SAFEWORD UNIX-SAFE

VERSION 3.1

30 June 1987

SUB-SYSTEM EVALUATION REPORT

ENIGMA LOGIC, INC.

SAFEWORD UNIX-SAFE VERSION 3.1

NATIONAL
COMPUTER SECURITY CENTER

9800 SAVAGE ROAD
FORT GEORGE G. MEADE
MARYLAND 20755-6000

June 30, 1987

CSC-EPL-87/002
Library No. S228,514

CSC-EPL-87/002
Library No. S228,514

FOREWORD

This publication, the Sub-system Evaluation Report, Enigma Logic, Inc., SafeWord UNIX-Safe Version 3.1, is being issued by the National Computer Security Center under the authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center." The purpose of this report is to document the results of an evaluation of Enigma Logic's SafeWord UNIX-Safe product. The requirements stated in this report are taken from Department of Defense Trusted Computer System Evaluation Criteria, dated December 1985.

Approved:

June 30, 1987

Eliot Sohmer
Chief, Product Evaluations
and Technical Guidelines
National Computer Security Center

ACKNOWLEDGEMENTS

Evaluation Team Members

James L. Arnold

Stephen F. Carlton

National Computer Security Center

9800 Savage Road

Fort George G. Meade, Maryland 20755-6000

CONTENTS

EXECUTIVE SUMMARY

SafeWord UNIX-Safe(1) (SafeWord) has been evaluated by the National Computer Security Center (NCSC). SafeWord is considered to be a security sub-system rather than a complete trusted computer system. Therefore, it was evaluated against a relevant subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria, dated December 1985. Specifically, the subset in this evaluation included identification & authentication (I & A) and audit.

The NCSC evaluation team has determined that SafeWord is capable of applying these security features to any IBM PC/AT(2) running under the XENIX(3) operating system. In addition to the standard XENIX login mechanism, SafeWord maintains user I & A by requiring each user to enter a user ID and then a valid response to the challenge subsequently issued by SafeWord. Audit records are generated and maintained for all login attempts. Each user is given two attempts to login before a disconnect occurs. The result of the two attempts, success or failure, is appropriately logged.

These security mechanisms can be maintained only if the code that implements them is protected from unauthorized modification. SafeWord includes tamper testing logic which is capable of detecting unauthorized modification. However, in the XENIX environment, the file system should be configured such that only a user logged in with root privilege can modify the SafeWord program and it's associated data files. This type of file structure is recommended in the associated documentation. In addition, to provide maximum assurance, every user of the system must be protected by SafeWord. Each non-SafeWord protected user account represents a way to bypass the SafeWord security mechanisms, thus defeating the purpose of the security package.

---

(1) SafeWord is a registered trademark of Enigma Logic, Inc. UNIX is a registered trademark of AT&T Bell Labs, Inc.

(2) IBM PC/AT is a registered trademark of the IBM Corporation.

(3) XENIX is a registered trademark of the MicroSoft Corporation.

INTRODUCTION

Background

On January 2, 1981, the Director of the National Security Agency was assigned the responsibility for increasing the use of trusted computer security products within the Department of Defense. As a result the DoD Computer Security Center was established at the National Security Agency. Its official charter is contained in DoD Directive 5215.1. In September 1984, National Security Decision Directive 145 (NSDD 145) expanded these responsibilities to include all federal government agencies. As a result, the Center became known as the National Computer Security Center (NCSC) in August 1985.

The primary goal of the NCSC is to encourage the widespread availability of trusted computer systems: systems that employ sufficient hardware and software integrity measures for use in the simultaneous processing of a range of sensitive or classified information. Such encouragement is brought about by evaluating the technical protection capabilities of industry- and government-developed systems, advising system developers and managers of their systems' suitability for use in processing sensitive information, and assisting in the incorporation of computer security requirements in the systems acquisition process.

The NCSC Computer Security Sub-system Evaluation Program

While the NCSC devotes much of its resources to encouraging the production and use of large-scale, multi-purpose trusted computer systems, there is a recognized need for guidance on, and evaluation of, computer security products that do not meet all of the feature, architecture, or assurance requirements of any one security class or level of the Criteria. The NCSC has, therefore, established a Computer Security Sub-system Evaluation Program.

The goal of the NCSC's Computer Security Sub-system Evaluation Program is to provide computer installation managers with information on sub-systems that would be helpful in providing immediate computer security improvements to existing installations.

Sub-systems considered in the program are special-purpose products that can be added to existing computer systems to increase some aspect of security and have the potential of meeting the needs of both civilian and government departments and agencies. For the most part, the scope of a computer security sub-system evaluation is limited to consideration of the sub-system itself, and does not address or attempt to rate the overall security of the processing environment. To promote consistency in evaluations an attempt is made, where appropriate, to assess a sub-system's security-relevant performance in light of applicable standards and features outlined in the Criteria. Additionally, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, a summary of this evaluation report will be placed on the Evaluated Products List.

This report will not assign a specific rating to the product, but will provide an assessment of the product's effectiveness and usefulness in increasing computer security.

PRODUCT EVALUATION

Product Overview

SafeWord UNIX-Safe (SafeWord) is a software package which, when implemented on any system running under XENIX, provides user identification and authentication (I & A) mechanisms, and auditing of these mechanisms (audit). These security mechanisms can be used either independently or as supplements to those already provided by the underlying operating system.

The SafeWord system is comprised of two programs, four data files, and individual hand-held, pseudo-random number (PRN) generating devices. The two programs provide the I & A and audit mechanisms and SafeWord maintenance utilities. Each program takes advantage of the setuid function provided by XENIX. When executing one of these programs, this function gives any user the privilege to access SafeWord files that would normally be inaccessible. However, the access is strictly controlled by each privileged program. The primary data file contains the SafeWord user database. Two others contain the successful and failed login audit records. The last data file is simply an index into the SafeWord user database. These files are only protected by the standard XENIX access controls (i.e., only a user operating with root privilege may access them). These controls make use of protection bits on each object in the system and have been shown to be vulnerable to penetration in the past. Finally, each SafeWord user is assigned a hand-held PRN device with which to produce a correct response to a given challenge. In addition, each hand-held device is assigned a system-unique key and, if applicable to the specific device, a personal identification number (PIN). The key is unknown to the user, while the PIN must be known so that he may use it to identify himself to the device.

Evaluation of Functionality

Identification and Authentication

After successfully passing through any I & A mechanisms that may exist in the underlying operating system, the user must pass through SafeWord. The SafeWord I & A mechanism is a challenge-response system. Although Safeword will accept an independent login identifier, it should be configured by the administrator to use the XENIX user identifier to ensure that the

XENIX user and Safeword user are the same. After getting the user identifier, SafeWord issues an apparently arbitrary numeric challenge and the user replies with the appropriate response. The appropriate response is obtained by entering the user's personal identification number, if applicable (i.e., if using DES X9.9 Decoder or PFX PassPort(1) a PIN is required), and the challenge into the user's hand-held PRN device. The device, in turn, uses a fixed algorithm to produce the response. If a PIN is not required (i.e., if using the standard Enigma Logic Decoder) Safeword should be configured by the administrator to require a fixed password.

The hand-held PRN devices, which are used to produce correct responses, are currently available in three forms(2): the standard Enigma Logic Decoder, the Atalla Technovations Data Encryption Standard X9.9 Decoder, and the Sytek PFX PassPort. SafeWord provides the SafeWord administrator with the capability of assigning any one of the devices available to each user. In any case, the secret key (seed) for each device must be associated with the corresponding user in the SafeWord database. When the user initiates login by entering his personal identifier, the SafeWord system can then look for the user's information in it's database and can determine which algorithm to use and the appropriate seed. Once the algorithm and seed are determined, SafeWord can then issue an answerable challenge in the form of a PRN.

On the SafeWord system there are two special users, Super and Master. The person using the userid Super is intended to be the primary SafeWord administrator. This user may delegate administrative functions to other users by giving specific users the privileges necessary to execute specific SafeWord utility functions (i.e., view usage log, view fail log, edit access file, create usage log, and create fail log). The Master user, the user possessing the Master Key, is responsible for installing the system and repairing any software problems. If the SafeWord user database were ever to be destroyed, the Master user would still be able to access and repair the system by means of the Master Key. The Master Key is actually coded into the SafeWord software and cannot be disabled.

---

(1) PFX PassPort is a registered trademark of Sytek, Inc.

(2) Enigma Logic has plans to support additional devices in the near future.

Audit

SafeWord provides audit capabilities for all accesses to the host machine. The audit data is broken down into a usage log and failed login attempts. The usage log maintains an audit trail that consists of a log of the machine's usage. The failed login record maintains a log of failed access attempts, providing the capability to detect users attempting to access the machine without authorization. The size of the audit trail buffers can be set at the time of creating a new set of buffers. Any administrator who has been given the privilege to create the usage and fail logs can do this.

Audit records maintained in the usage log contain the time, date, user ID, and whether the login attempt was successful or not. Audit records maintained in the failed login log contain the time, date, user ID, reason for failure, challenge issued, and response given.

Evaluation of Documentation

The SafeWord UNIX-Safe documentation package consists of three manuals: the SafeWord UNIX-Safe Installation Guide rev. 1.0, Nov. 1986; the SafeWord IDUTIL Supervisor Guide, rev. 4, Jan. 1987; and the SafeWord ID User's Guide, rev. 2, Feb. 1986. It should be noted that these documents are generic to most versions of SafeWord, with the exception of the UNIX-Safe installation guide. As a result, the evaluation team found that some specifics, regarding our test system, were not documented in these manuals, and contact with Enigma Logic was required to clarify them(1). In addition, the version of SafeWord evaluated provided features not described in the version of the documentation that was reviewed (e.g., the SafeWord administrator function to delegate administrative privilege). Enigma Logic is currently developing documentation for version 3.1 of SafeWord UNIX-Safe. Otherwise, the documentation was found to be complete and accurate, except as noted later in this report.

---

(1) Enigma Logic has plans to correct this situation in subsequent editions of SafeWord documentation.

SafeWord UNIX-Safe Installation Guide

This thirteen page guide is intended for the individual responsible for installing the system initially. It includes the following sections:

Introduction

The introduction lists the major components of the SafeWord System, and clarifies some of the notation used in the document.

Section 1: Security and the UNIX Operating System

This section presents an overview of the interface between SafeWord and the existing UNIX-like operating system.

Section 2: Installation of UNIX-Safe

This section presents detailed instructions for installing the SafeWord System.

Section 3: Adding New Users

This section explains how new users are added to the SafeWord System.

SafeWord IDUTIL Supervisor Guide

This forty three-page guide is intended for the individual(s) responsible for administrating and maintaining the SafeWord system. It includes the following sections:

Introduction

The introduction lists the major components of the SafeWord System, and clarifies some of the documentation conventions used in the document.

Section 1: SafeWord ID Product Description

This section presents a complete description of the SafeWord System.

Section 2: Accountable Domains and Their Component Parts

This section presents detailed descriptions of the various modes in which the SafeWord System can operate.

Section 3: The IDUTIL Files

This section describes the resource files that are used by the IDUTIL program.

Section 4: Startup

This section explains how the ID and IDUTIL programs are used by the system.

Section 5: The IDUTIL Main Menu

This section outlines the functions available to the SafeWord system administrator.

Section 6: Training and Administration

This section explains how to organize the administration of the SafeWord System.

SafeWord ID User's Guide

This sixteen-page guide is intended for the end user of the SafeWord system. It includes the following sections:

Introduction

The introduction lists the major components of the SafeWord System, and clarifies some of the notation used in the document.

Section 1: SafeWord ID Description

This section presents a user's overview of the SafeWord System.

Section 2: Daily Operation Within the Accountable Domain

This section describes the effects of the SafeWord accountable domain on the typical user.

Appendix 1: Glossary of SafeWord Terms

An index of SafeWord terminology and definitions.

THE PRODUCT IN A TRUSTED ENVIRONMENT

The rapid introduction of office automation products into the workplace has brought with it the need to protect and control access to data stored on these systems. Initially, protection was provided solely by the individual who maintained physical possession of his own data and operating system on diskettes, giving a reasonably high assurance of maintaining data and code integrity. These procedural controls isolated users, and thus prevented intentional or accidental access to other users' data. Other security mechanisms were not deemed necessary since the user was only able to inflict damage to his own data or operating system.

The advent of inexpensive and reliable hard disk drives introduced new security implications. In a working environment where it was common to have many users share the same PC, they now shared and stored their data on the same hard disk memory unit. In this environment, users no longer had the assurance that their data was protected from unauthorized access, or even that the underlying operating system had not been subverted. Procedural controls could no longer provide the adequate user isolation and controlled sharing necessary for this environment.

The Enigma Logic SafeWord UNIX-Safe (SafeWord) product is designed to help add assurance in the protection of individual users' data on the XENIX operating system. This is achieved by requiring that each user identify and authenticate himself before being granted access to the machine and, hence, to the data. In addition, access attempts are audited, providing a capability to detect attempts to gain unauthorized access to the system and to enforce individual user accountability.

When configured as tested, SafeWord provides effective identification, authentication, and auditing mechanisms. It is recommended that, just as tested, SafeWord be configured to pass the XENIX login identifier to the SafeWord login mechanism to ensure that a single user is being authenticated by both mechanisms. In addition, should users be using hand-held pseudo random number devices that do not require personal identification numbers (i.e., standard Enigma Logic Decoder), SafeWord should be configured to require a fixed password.

PRODUCT TESTING

Test Procedure

Testing represents a significant portion of a sub-system evaluation. The test suite used by the evaluation team tested SafeWord identification, authentication (I & A), and audit mechanisms. This functional test suite focused upon those security features identified in the Safeword IDUTIL Supervisor Guide. The test suite consisted of three main sections. The first part focused primarily on audit. The second part involved an attempt to access and/or subvert the information in the SafeWord data files and an attempt to disable the SafeWord identification program. The last part was directed at functional testing of the SafeWord utility program.

All tests were performed using Safeword executing on an IBM PC/AT under the XENIX (version 2.0) operating system. Although SafeWord provides several configuration options, most of the testing was performed with SafeWord configured by its defaults, with the following exception. When configured by default, the XENIX and SafeWord login procedures are completely independent. Thus, once a user gets past the XENIX login mechanism, any valid SafeWord user may then login normally, even if he is not the same user that logged in under XENIX. For our testing, SafeWord was configured such that the XENIX user identifier was passed on to SafeWord, ensuring that both the XENIX user and the SafeWord user were the same. This configuration was easily achieved using the menu options provided by SafeWord.

Test Results

The following list of test results include only those that the evaluation team believes are security relevant.

Audit

Accesses to the SafeWord utility program are recorded in the audit files, just as if the user were logging in to the system. However, no distinction is made between the two cases in the audit records.

It was determined that, in the event of an audit file overflow, the individual audit records are handled on a first-in first-out basis and the old audit records are lost. The maximum size of the audit files is controlled by the SafeWord administrator, but can only be altered by replacing the existing files with new files of the desired size. There is no warning of an imminent audit record file overflow.

SafeWord Data File Integrity

It was determined that the SafeWord data files could only be accessed by a user executing with XENIX root privilege. In addition, SafeWord encrypts the data files for additional protection from disclosure and undetected modification. The encryption algorithm was not evaluated by the evaluation team. The SafeWord programs are protected by XENIX, such that only a user with XENIX root privilege can modify them.

SafeWord Utility Functional Testing

The utility program is completely menu driven and was found to be functionally correct and user friendly.

☆ USGPO 1989- 622-523/10075

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No 0704-0188

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS NONE
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT DISTRIBUTION UNLIMITED
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) CSC-EPL-87/002	5. MONITORING ORGANIZATION REPORT NUMBER(S) S228,514
6a. NAME OF PERFORMING ORGANIZATION National Computer Security Center 6b. OFFICE SYMBOL (If applicable) C12	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State, and ZIP Code) 9800 Savage Road Ft. George G. Meade, MD 20755-6000	7b. ADDRESS (City, State, and ZIP Code)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code)	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO / WORK UNIT ACCESSION NO.

11. TITLE (Include Security Classification)

(U) Sub-system Evaluation Report, Enigma Logic, Inc. SafeWord UNIX-Safe Version 3.1

12. PERSONAL AUTHOR(S)
James L. Arnold, Stephen F. Carlton

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
Final	FROM _____ TO _____	870630	20

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	NCSC TCSEC sub-system Enigma Logic Audit I&A SafeWord UNIX-Safe Identification Authentication

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

The Enigma Logic, Inc. SafeWord UNIX-Safe Version 3.1 product was evaluated against identification and authentication and audit requirements of the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), dated December 1985. The product is a software package which, when properly installed, provides additional assurance through the implementation of the features listed above.

This report documents the findings of the evaluation.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION	
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	UNCLASSIFIED	
22a. NAME OF RESPONSIBLE INDIVIDUAL LTC Lloyd D. Gary, USA	22b. TELEPHONE (Include Area Code) (301) 859-4458	22c. OFFICE SYMBOL C/C12

DD Form 1473, JUN 86 *Previous editions are obsolete.* SECURITY CLASSIFICATION OF THIS PAGE

UNCLASSIFIED